**SUBJECT: SYSTEM AND NETWORK ADMINISTRATION**

**CLASS: BSIT 5TH SS1**

**TEACHER : MISS MISBAH JABEEN**

**GROUP MEMBERS**

**NAME : MUHAMMAD FAISAL**

**ROLL NO. : BSIT51F22S019**

**NAME: SHAHZAIB MALIK**

**ROLL NO. : BSIT51F22S048**

**Project: Investigating cctv\_logs in Splunk**

Splunk is a powerful platform for searching, monitoring, and analyzing machine-generated big data via a web-style interface. It is widely used for operational intelligence, IT operations, security, and data analytics.

**Project is based on following scenario**.

scenario presents an intriguing mystery involving unauthorized access to a CCTV system, culminating in the deletion of footage. Let’s walk through the case systematically to explain the situation, the investigation process, and the resolution:

**Background**

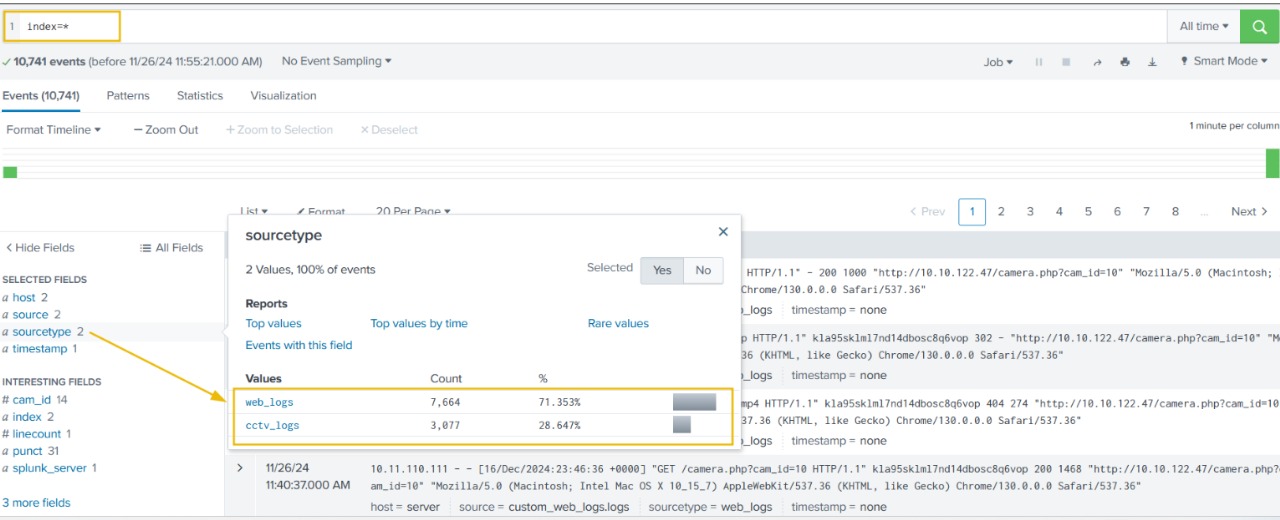
The peaceful town of Sui is thrown into chaos when Faisal discovers that the main server has been disconnected from the network. Sui’s security company, WareSec&Aware, claims that no one accessed the data center, yet the CCTV streams are mysteriously missing. The cameras' ownership lies with Byte, Shahzaib’s trustworthy dog, ensuring impartiality. Despite Byte’s innocence, Faisal is distraught as her initial searches yield garbled logs that cannot reveal what happened.

**Investigation Begins**

Faisal turns to Farhan and Shahzaib for help. They rely on Splunk, a powerful Security Information and Event Management (SIEM) tool, to analyze the logs. Here's the step-by-step breakdown of how they uncover the truth:

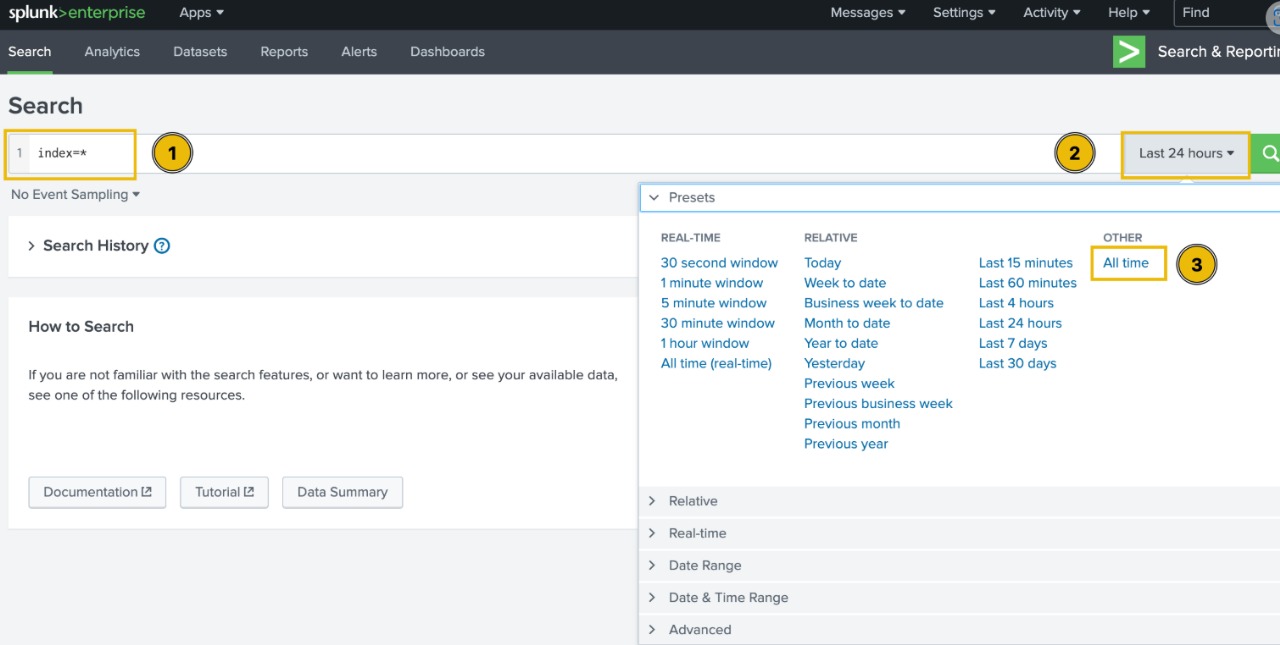
**1. Understanding the Logs**

The logs consist of two datasets:

**web\_logs**: Related to web activity, such as IP addresses and web server connections.

**cctv\_logs:** Contains application logs for the CCTV system, detailing events like logins, video downloads, and footage deletions.

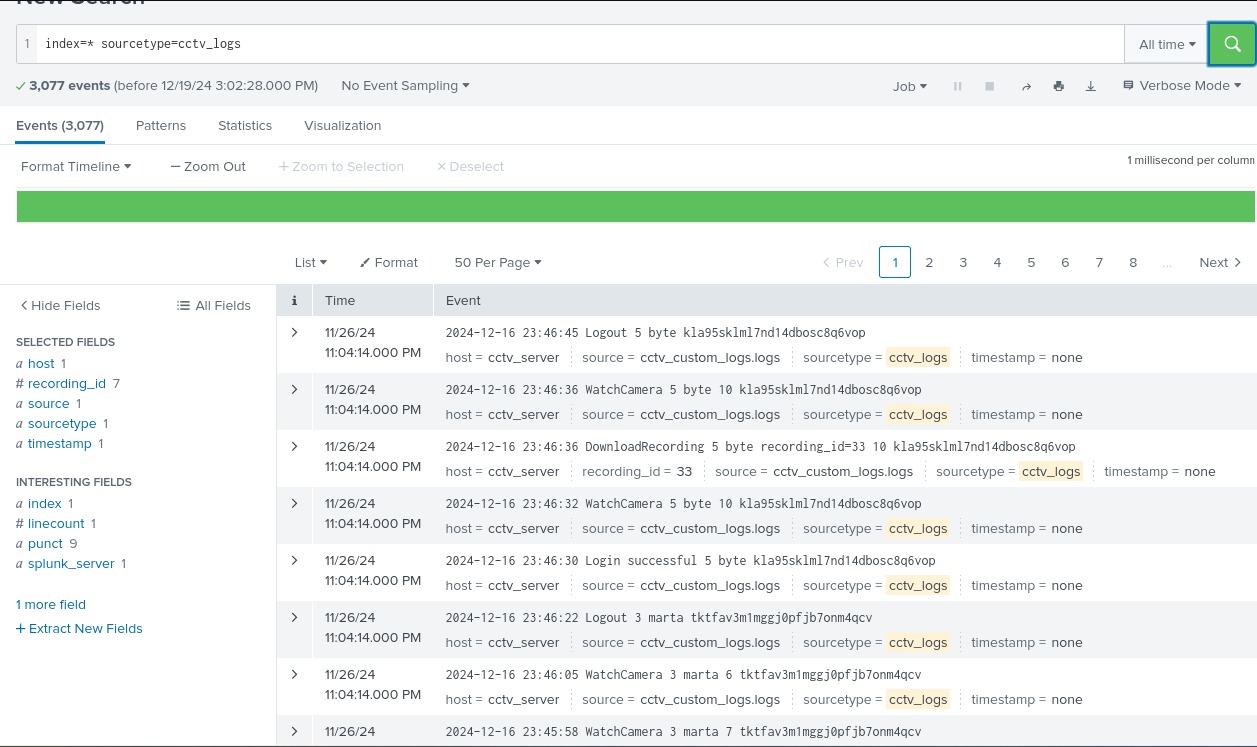
Type **index=\*** in the search bar to show all ingested logs. Note that we will need to select **All time** as the time frame from the drop-down on the right of the search bar.

****

**Examining CCTV Logs**

Let's start our investigation by examining the CCTV logs. To do so, we can either click on the corresponding value for the **sourcetype** field, or type the following query in the search bar:

**index=\* sourcetype=cctv\_logs**

****

**2. Parsing the Logs**

The investigation faces its first hurdle: the logs are poorly formatted, making them unreadable. Splunk cannot directly extract meaningful fields. To fix this:

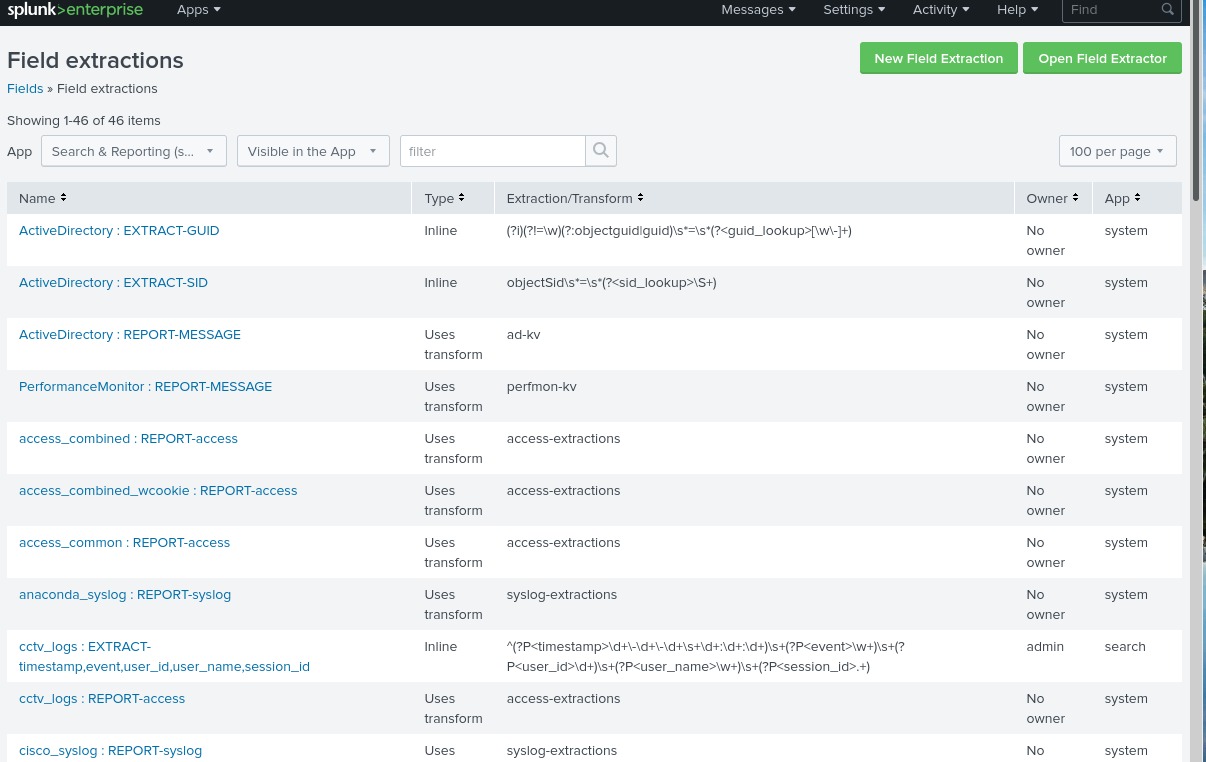
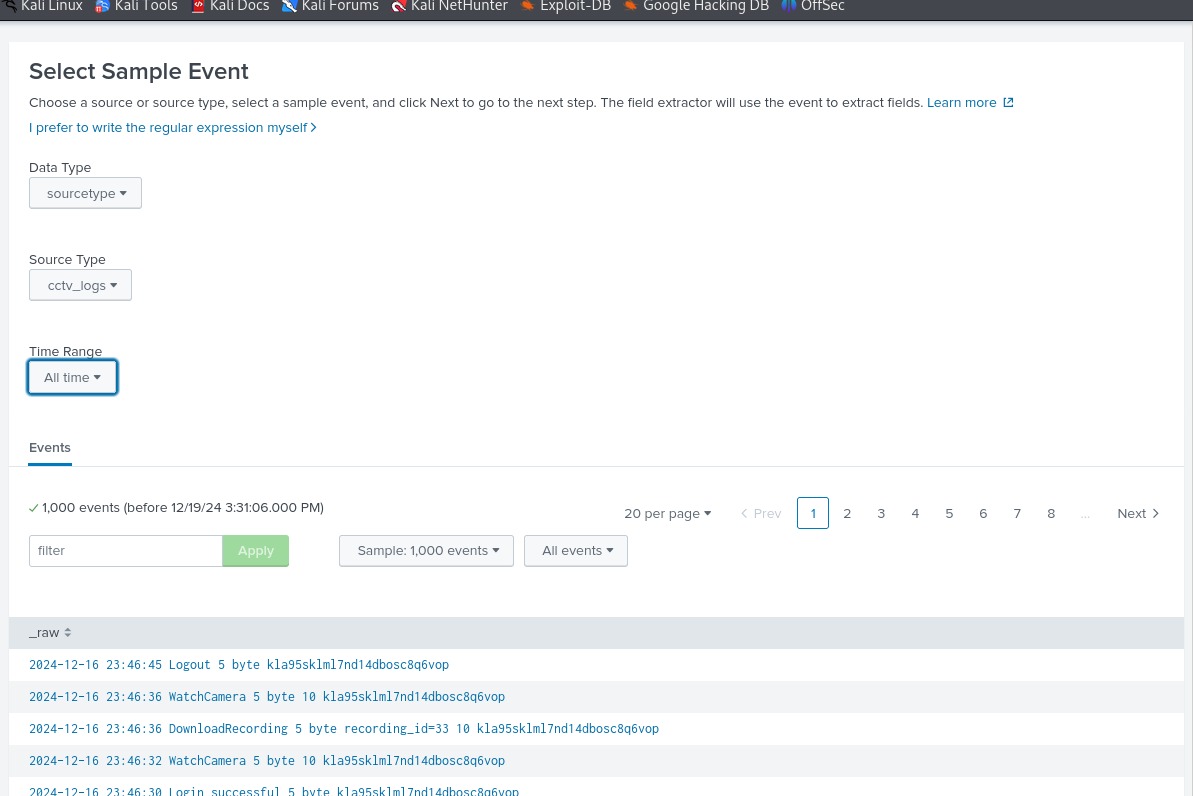
**Fixing the Problem**

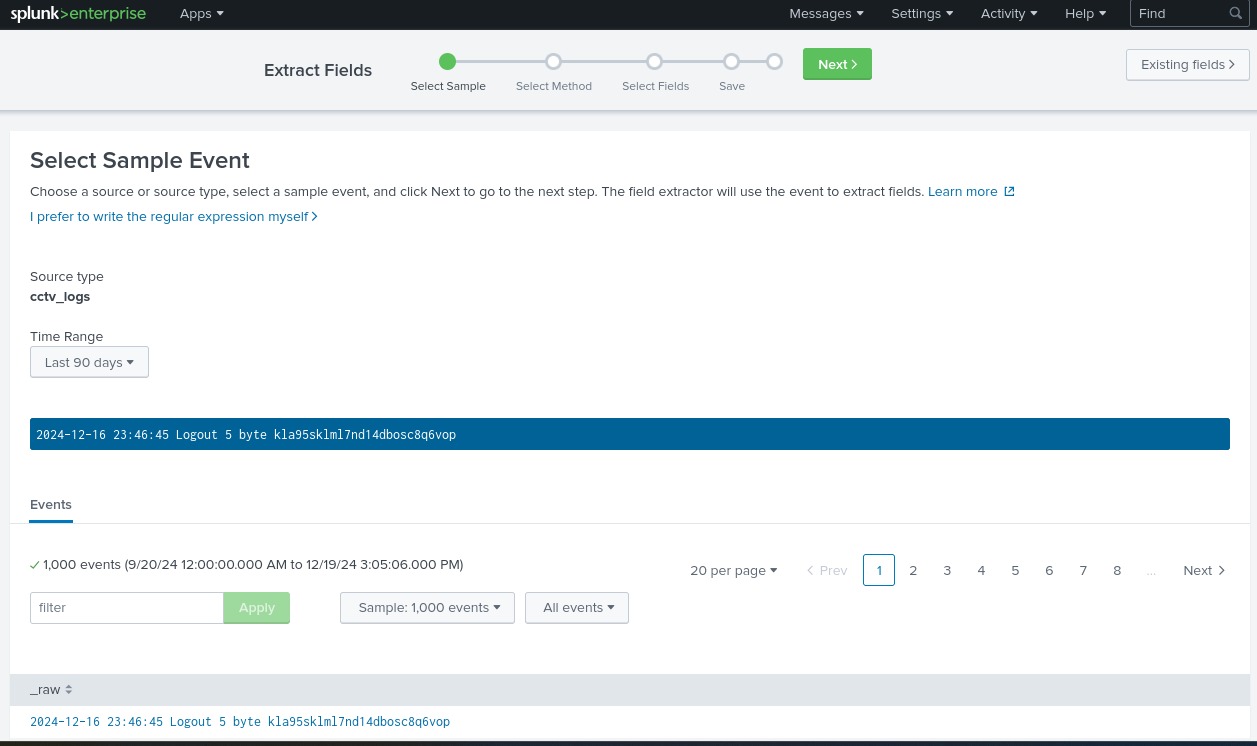
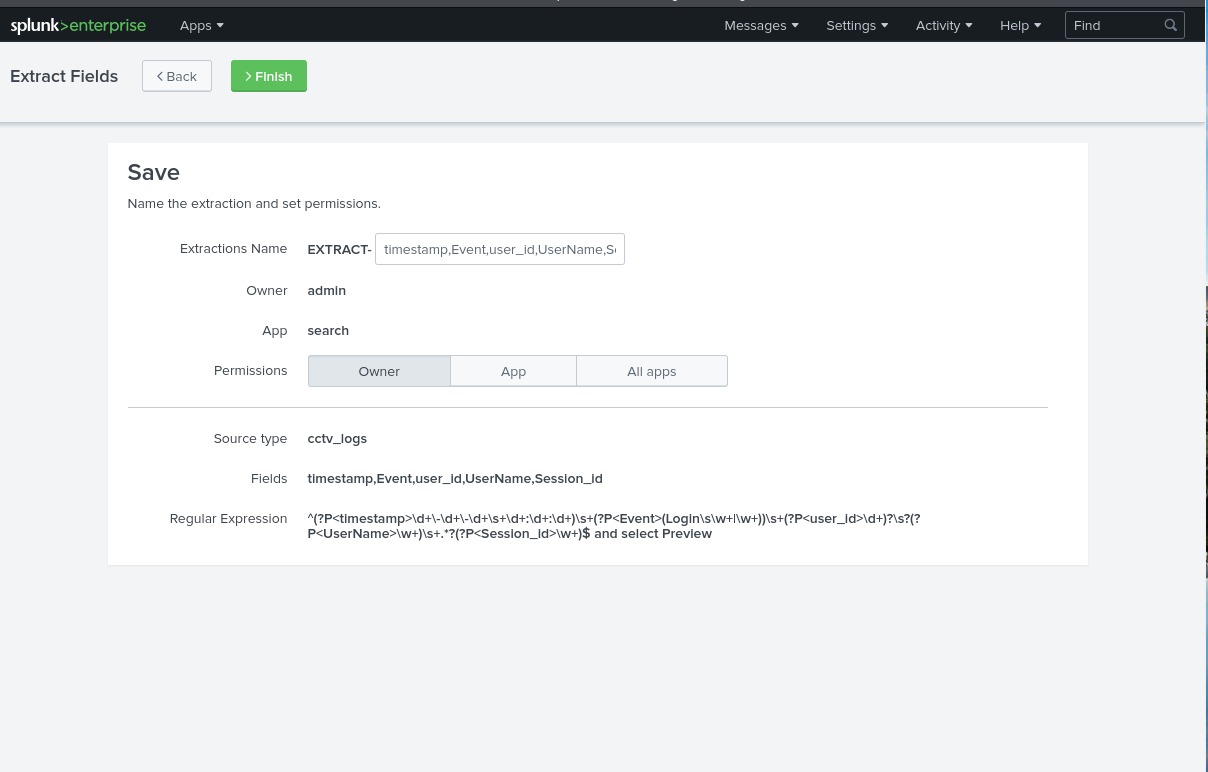
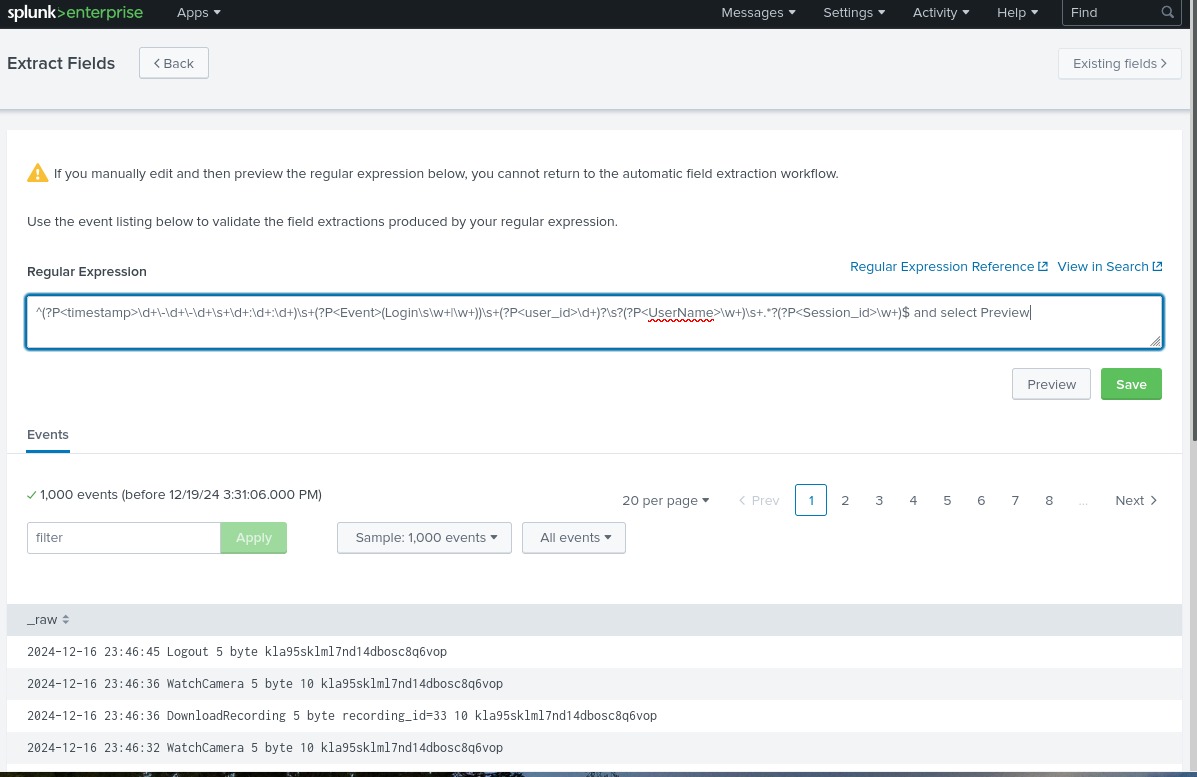
Before analysing and investigating the logs, we must extract the relevant fields from them and adjust the timestamp.

**Parsing the Logs**

The investigation faces its first hurdle: the logs are poorly formatted, making them unreadable. Splunk cannot directly extract meaningful fields. To fix this:

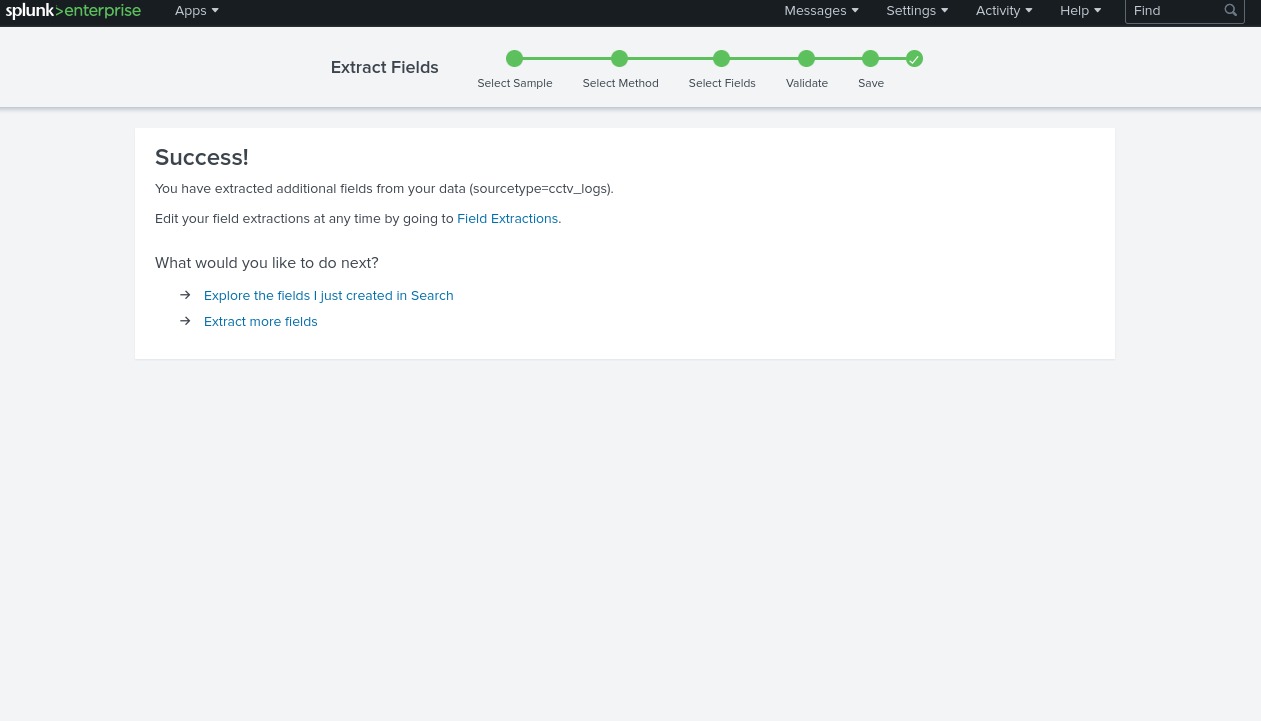
The team uses field extraction in Splunk to parse essential components (e.g., timestamp, event, user ID, session ID).

A custom regular expression (regex) is created to standardize and extract fields across varied log formats.



**REGEX**:” ^(?P<timestamp>\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2}) (?P<Event>\w+( \w+)?) (?P<user\_id>\d+)? (?P<UserName>\w+) .\*?(?P<Session\_id>\w+)$”

 Click on the **Explore the fields I just created in Search**.

Now that we can observe that all fields are being extracted as we wanted, let's start investigating the logs.

**Investigating the CCTV Footage Logs**

Now that we have sanitized and properly parsed the logs, it's time to examine them and find the culprit.

**Summary of the CCTV Feed**

After examining the CCTV feed logs, we can create a mental picture of the information these logs provide us. A brief summary of these logs is:

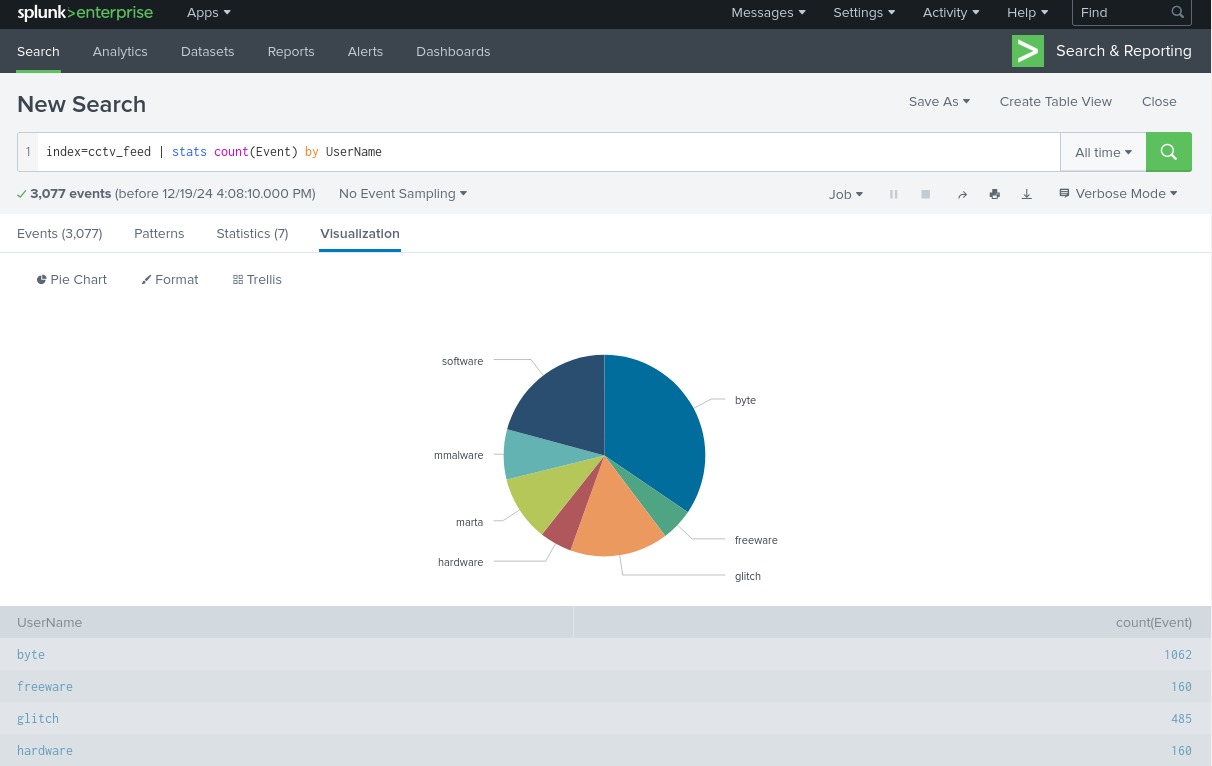
* These logs contain the successful and failed login attempts from various users.
* They contain a few failed login attempts, which looks suspicious.
* They contain information about the CCTV footage being watched and downloaded.

**Event Count by Each User**

Let's use the following search query to see the count of events by each user:

**index=cctv\_feed | stats count(Event) by UserName**

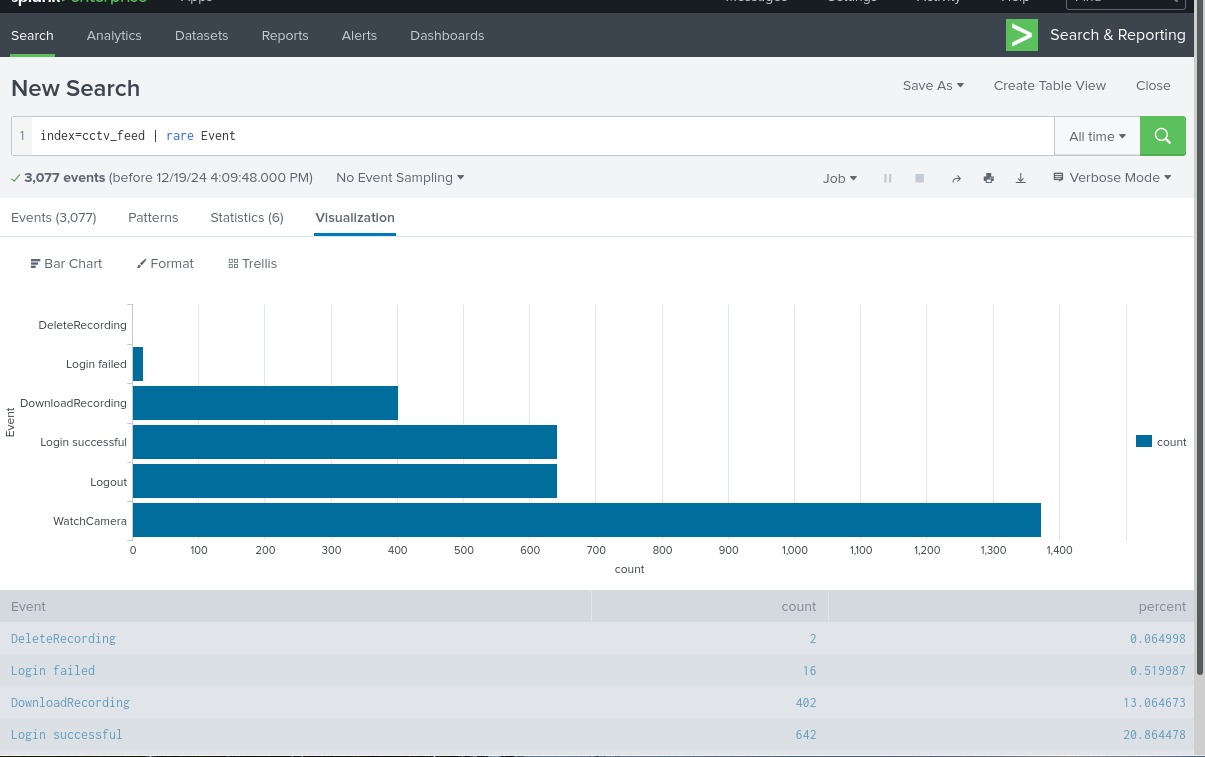
We can easily visualise this data by first clicking on **Visualization** below the search bar, then change the visualisation type from **Bar Chart** to **Pie Chart**.



**Examining Rare Events**

Using the following search query, let's look at the events with fewer occurrences in the event field to see if we can find something interesting:

**index=cctv\_feed | rare Event**



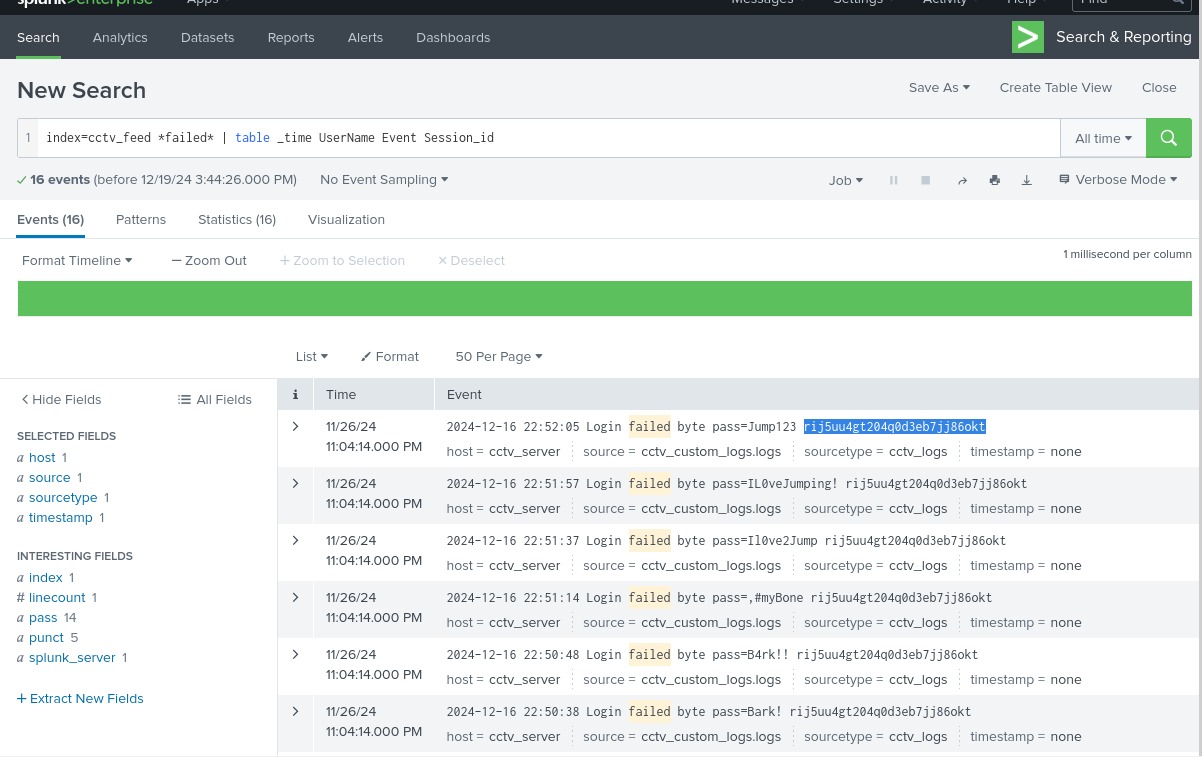
**Analyzing Suspicious Activity**

Once the logs are parsed, Farhan and Shahzaib notice:

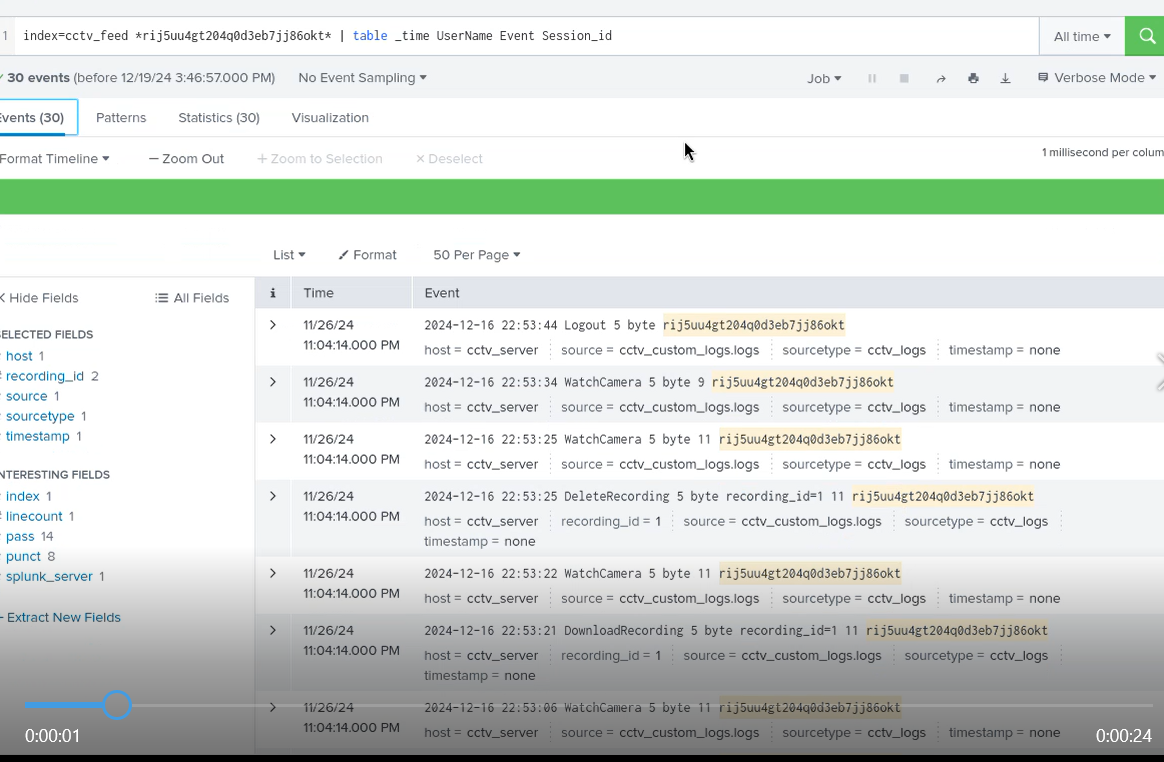
**Failed Login Attempts**: Multiple unsuccessful attempts suggest brute force attacks.

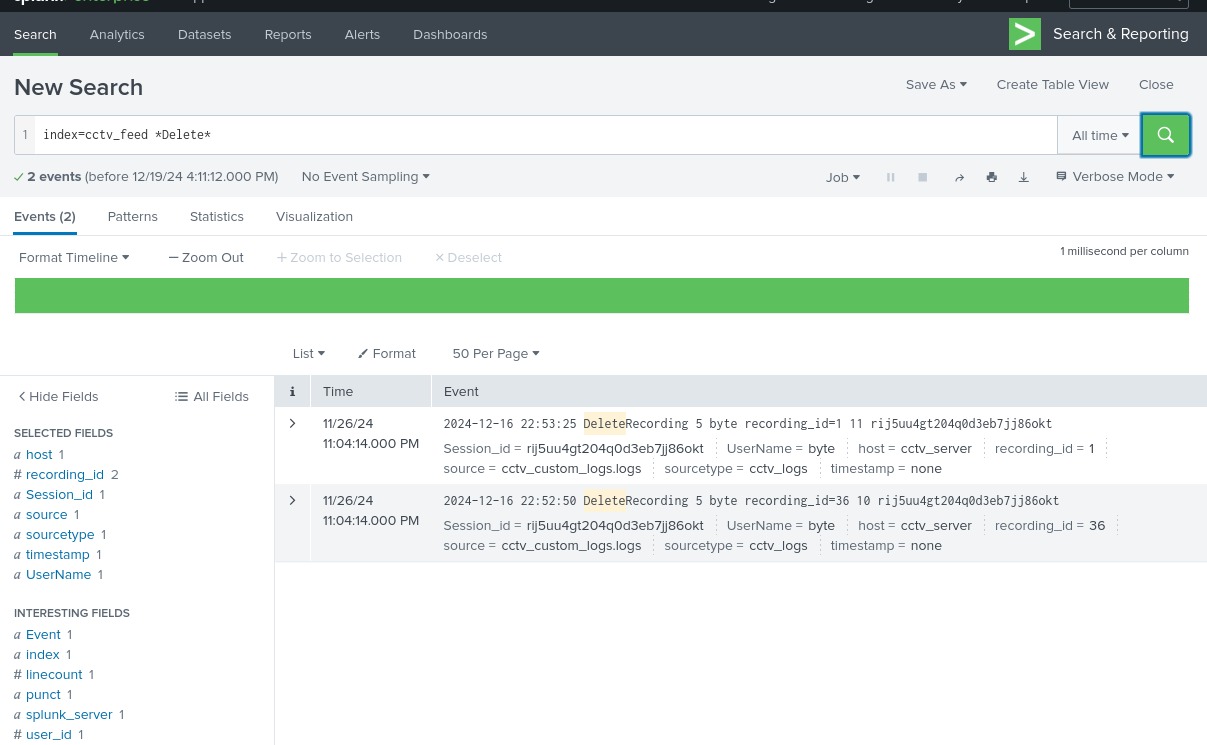
It looks like we have a few attempts to delete the recording and a few failed login attempts. This means we have a clue. Let's now examine the failed login attempts first:

**index=cctv\_feed \*failed\* | table \_time UserName Event Session\_id**

Copy the highlighted session\_id and replace it with the failed in the seacrch place.

**index=cctv\_feed \*session\_id\* | table \_time UserName Event Session\_id**



Let's see how many events related to the deletion of the CCTV footage were captured.

**index=cctv\_feed \*Delete\***

Good. We have some comprehensive information about the attacker and his notorious activities.

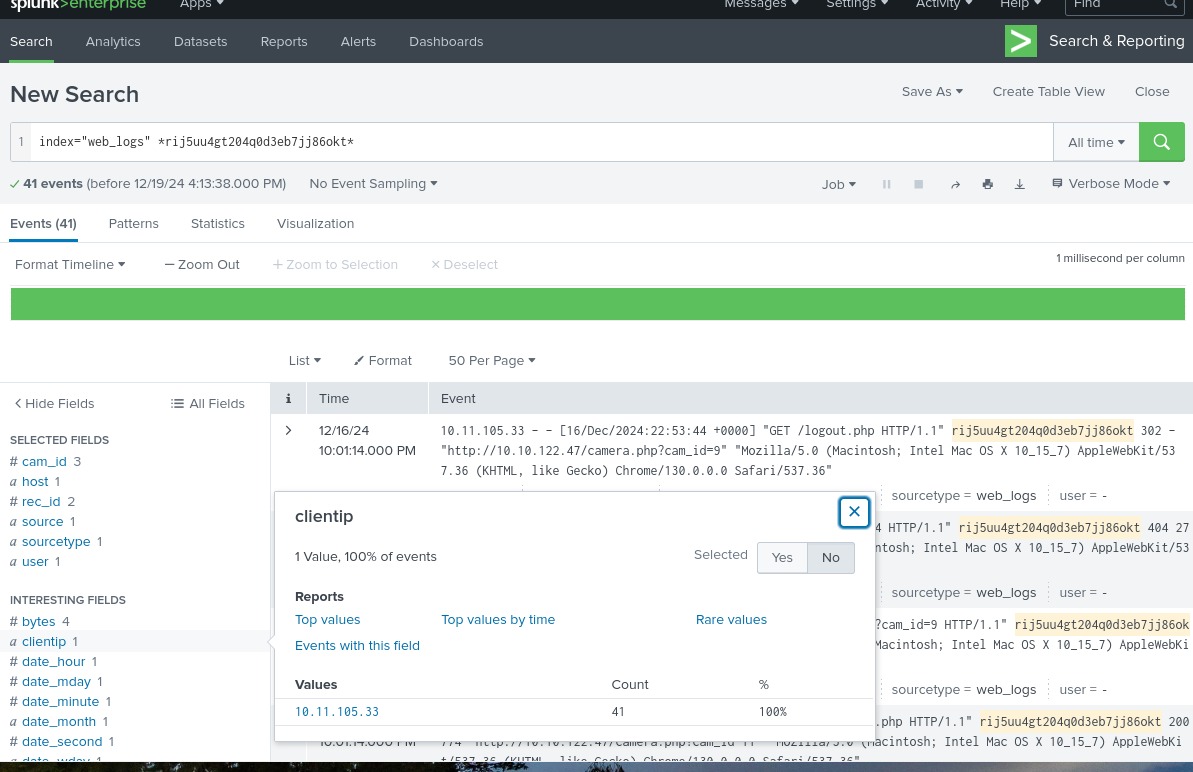
The attacker gained access after multiple failed attempts.

They downloaded several camera streams.

Finally, they deleted the footage to cover their tracks.

**Correlating With Web Logs**

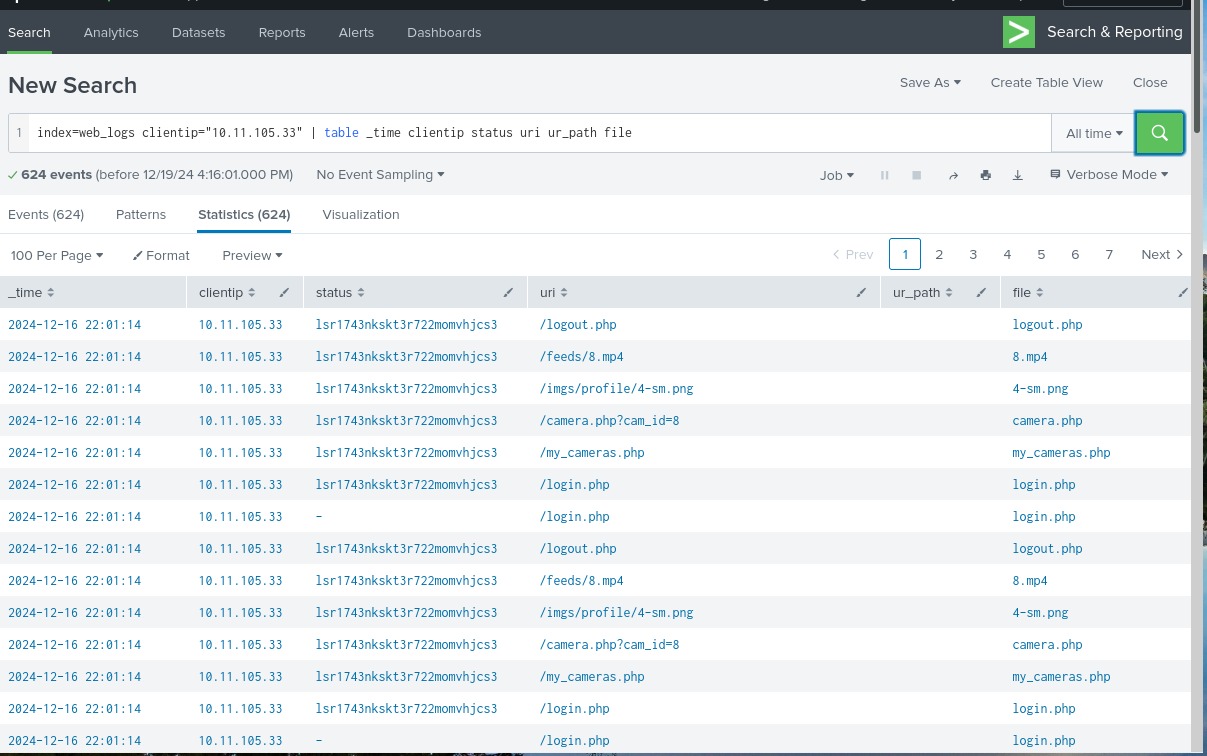
The team then switches to the web\_logs dataset to trace the attacker's IP address.By examining logs linked to the suspicious session ID: Let's use the information extracted from the earlier investigation and correlate it with the web logs.



Now we have got the ip address of the user by session\_id navigating through the client\_ip field in the fields tab.

Let's create a search to observe what kind of activities were captured associated with the IP and these session IDs.

**index=web\_logs clientip="10.11.105.33" | table \_time clientip status uri ur\_path file**

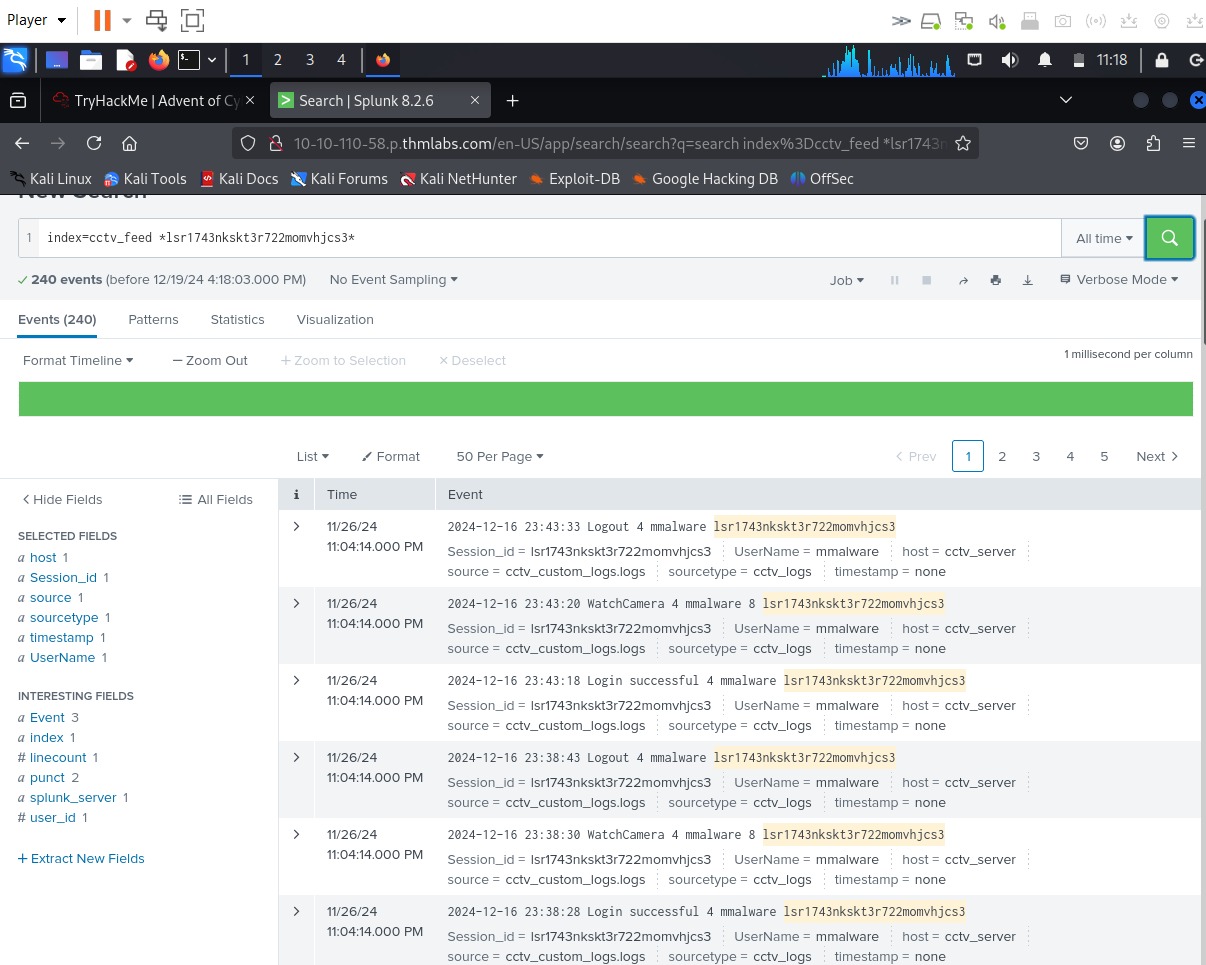


Looking closely, we can see logout events when the session ID was changed. Can we correlate these session IDs in the cctv\_feeds logs and see if we can find any evidence?

**Connecting the Dots:**

Let's go back to **cctv\_feed** and use these session IDs associated with the IP address, as shown below:

**index=cctv\_feed \*lsr1743nkskt3r722momvhjcs3\***

Great, we were able to locate the user name associated with the attack. Now that we have identified the user, let's summarise our investigation.

From the output, it seems the following was the timeline of the attack:

* Attacker bruteforce attempt on various accounts.
* There was a successful login after the failed attempts.
* Attacker watched some of the camera streams.
* Multiple camera streams were downloaded.
* Followed by the deletion of the CCTV footage.
* The web logs had an IP address associated with the attacker's session ID.
* We found two other session IDs associated with the IP address.
* We correlated back to the cctv\_feed logs to find the traces of any evidence revolving around those session IDs, and found the name of the attacker.

**THANK YOU**